International Journal of Grid and Distributed Computing
Vol. 9, No. 9 (2016), pp.205-212
http://dx.doi.org/10.14257/ijgdc.2016.9.9.18

Multilevel Authentication Scheme for Cloud Computing

Sara Alfatih Adam[1] , Adil Yousif[2] and Mohammed Bakri Bashir[3]

University of Khartoum[1], University Science & Technology-Sudan[2], Shendi University-Sudan[3]

Abstract

Cloud Computing is a new technology that allows access to applications as utilities over the internet. Cloud computing environment provides a great flexibility and availability of computing resources at a lower cost. However, it brings new security concerns mainly when users understand exactly how a process is running. One of the main important challenges in cloud computing is data security, as users need to access data they share securely. So the main problem is how to employ an effective authentication procedure for ensuring data security and preventing unauthorized users to access the authorized user's data. This paper identifies the security issues of single level authentication and the problem of single password. This study proposed a new security mechanism for cloud computing based on multilevel authentication. The proposed scheme aimed to enhance the security and authentication process in cloud computing. The proposed scheme consists of three level of authentication, and the data will be splitting on this level depending on the sensitivity to confidential (C), secret (S), and top secret (TS). Data at level (C) have the lowest sensitivity. The user at this level has single textual password to access this level data. The user at level (S) has two passwords, textual and biometrics password to access this level and the lower level. User at level (TS) has three password textual, biometrics password and image sequencing password. The data at this level is the more sensitive data so it is encrypted using RSA algorithm before storing in cloud database. The results of the proposed multilevel authentication for cloud computing were promising.

***Keywords**: Authentication, Multilevel, Security, Cloud Computing*

1. Introduction

Cloud computing is a new technology that move the computation process from desktop computers to cloud providers through the internet[1]. Cloud computing provides computer infrastructures, platforms and software as services. This model decreases the computation cost and make organizations focus on their businesses. Three types of services are offered by cloud providers. These types are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In Software as a Service (SaaS), cloud providers provide software applications as services for clients. In Platform as a Service (PaaS) cloud providers provide platforms for clients so clients can develop their own applications on those platforms. In Infrastructure as a Service (IaaS), cloud clients request computer hardware such as processing unit, storage devices and network components as services[2, 3].

One of the main benefits of cloud computing is releasing cloud clients from the concerns about processing details and how data will be handled. However, moving to cloud brings new challenges and concerns regarding security and privacy [4-6]. Authentication of cloud users represents a critical issue in cloud computing security. Several cloud providers use single level authentication scheme as shown in Figure 1, such as simple text password for clients to access cloud services.

ISSN: 2005-4262 IJGDC

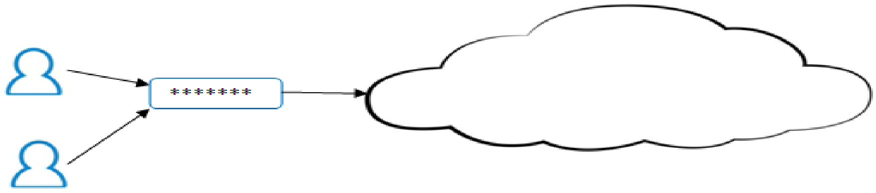

Figure 1. Single Level of Authentication for Cloud Computing

Other cloud providers employ graphical password third party authentication and biometric authentication. However, most of these models have limitations and do not work well if they used in single level authentication scheme. So the main problem challenge in cloud computing is how to perform a proper authentication procedures for ensuring data security and preventing unauthorized users to access the confidential data. The objective of this research is to propose a new model for cloud security that enhances authentication system based on multilevel authentication.

This paper has six sections. Section two describes the related works. Section three illustrates the multilevel security. Section four describes the proposed scheme. Section five presents the results and discussions and we concluded in section six.

2. Related Works

Yassin, A. A., H. Jin, et al in [7] developed a new a scheme for cloud authentication that depends on One-Time Password (OTP), Asymmetric Scalar-product Preserving Encryption (ASPE) and RSA digital signature as two factors. The model proposed in [8] is based on strict authentication system by introducing multi-level authentication technique which generates and authenticates the password in multiple levels to access the cloud services. The limitation of these methods is they use the same password at different level of authentication. The researchers in [9] apply a new framework for secure cloud authentication using tenants identification model. To overcome Denial-of-Service attack and to insecure password change Jaidhar C. D proposed an enhanced mutual authentication scheme for cloud architecture [10].

3. Multilevel Security

Multilevel security is a security discipline in which more than one security control is used to protect system security. Mandatory access control (MAC) is a scheme that prevents unauthorized clients from accessing objects that have sensitive information[11].

3.1 Multilevel Database Security

One of the main applications for mandatory access control is multilevel security (MLS), which has been built mainly for network, database and computer systems that have highly sensitive information[12].

Each item in multilevel security is defined as an object and has a security class level. Moreover, each user is considered as a subject and also has a security class level. In multilevel security a label is the class level of an object or a subject X and is denoted as L(X). Different access control are available for multi level security, Bell–LaPadula is a main one [11]. Bell–LaPadula model has three rules. The first one is: a user x is granted a read access to an object o only if L (x) is higher than or equal to L (o). The second rule is: a user x is granted a write access to an object o only if L(x) is less than or equal to L(o). The third rule is: a user x is granted a write access to an object o only if L(x) is equal to L (o). Bell–LaPadula model aims to prevent a subject with lower level from accessing a higher level object and this called no read-up discipline.

3.2 Multilevel Authentication System

Cloud providers offer internet based on-demand data storage services to clients or tenants. In this scheme, client's databases are stored remotely in the cloud provider data centers. The security of client's databases is based on the security controls employed by the cloud providers[13]. Cloud providers use single level authentication to allow clients access their data securely. Simple text password, biometric authentication, third party authentication, and graphical password are the main single level authentication used in cloud computing [14].

Each single level authentication scheme has limitations and drawbacks if scheme is used alone. Textual password authentication model is easy to break and vulnerable to dictionary and brute force attacks. For small cloud services, third party authentication is not recommended. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. Nevertheless, some graphical password mechanism is time and memory consuming. Bio-metric authentications scheme such as, fingerprints, hand geometry, face recognition, and voice recognition has been used for cloud services authentication. One of the key challenge and disadvantage of applying biometrics is its intrusiveness upon a client's personal characteristic. Furthermore, biometric scheme require a special scanning device to validate users characteristic, which is not appropriate for internet users [14]. In experiment done by Klein, after he collected passwords of nearly 15000 accounts that had alphanumerical passwords and he reached the following observation: 25% of the passwords were guessed using a small yet well-formed dictionary of 3 × 106 words. Furthermore, 21% of the passwords were guessed in the first week and 368 passwords were guessed within the first 15 min[15].

Single level password based authentication are not secure enough and are suspected to various attack such as dictionary attack, brute force attacked and shoulder surfing attack. Once malicious user logs into account he has full access to all services of registered user. Currently no cloud service provider has implemented further security measures with this models to protect services available for registered user once user has logged in. There is serious issue in sharing scheme. Security measure applied to protect shared file are not up to the mark. Once the file is shared with the other user, it sends a link to other user so that he can access the file but this link is universal.

4. The Proposed Multilevel Authentication Model for Cloud Computing

The aim of this research is to propose a new scheme that provides higher security level for cloud services. The proposed scheme is based on a combination of the concept of multilevel security (MLS) and the multilevel authentication. The proposed scheme consists of three levels of security and three level of authentication from lowest to highest. While users in the lowest level have one password, textual password, the users in the second level have two passwords, textual and biometrics password. When the degree of sensitivity of data increased the need for protection is becoming more crucial. In this scheme the important data exists at the third level with three passwords for users to login and retrieve their data as described in Figure 2.

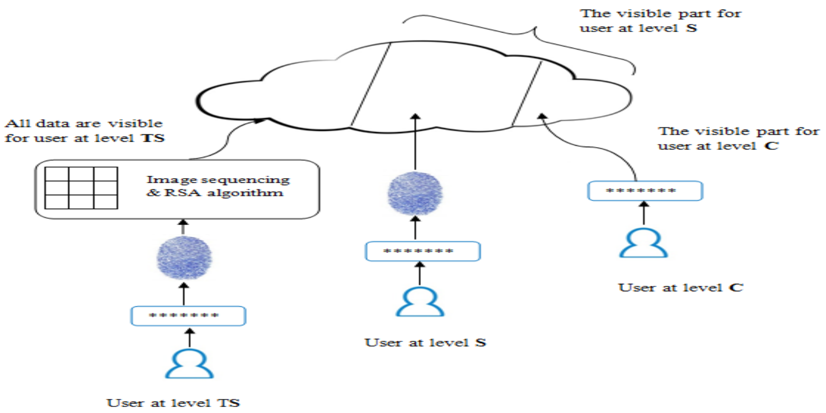
The visible part for user at level S
All data are visible for user at level TS
The visible part for user at level C
Image sequencing & RSA algorithm
****
****
****
User at level C
User at level S
User at level TS

Figure 2. The Proposed Scheme based on Multilevel of Authentication

In the proposed scheme multilevel security means locating the data at different levels of secrecy, the data may exist in one institution but it varies in the degree of confidentiality and its importance. The multilevel security hierarchy in the proposed scheme has three levels of increasing sensitivity. These levels, from lowest to highest, are confidential (C), secret (S) and top secret (TS) as shown in Figure 3. Users who need to access data should have the appropriate security access correspond to the classification level.

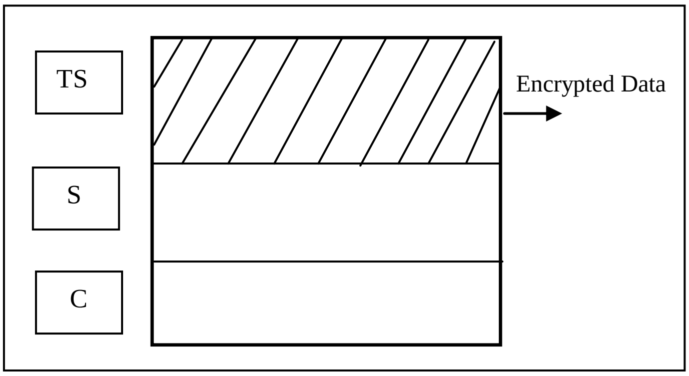

Figure 3: Multilevel Authentication Scheme

The data is divided based on data confidentiality into three levels: C (confidential) Level: Data in confidential level have lowest security; each authorized user in this level has only one password to access his data. When the user enters the password he can read and write the data within this level as described in Figure 4.

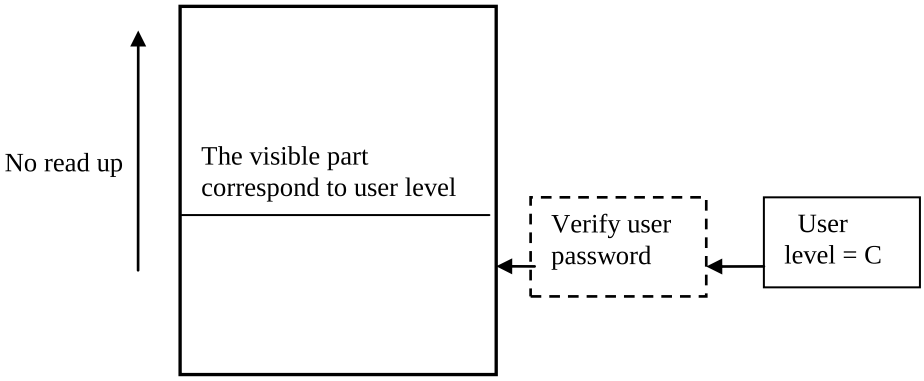

Figure 4. User at Level C

In S (secret) level, the users have the ability to read data with level C and data in their level but they are not allowed to write in the lower level. Any user in this level has two passwords for more security as shown in Figure 5.

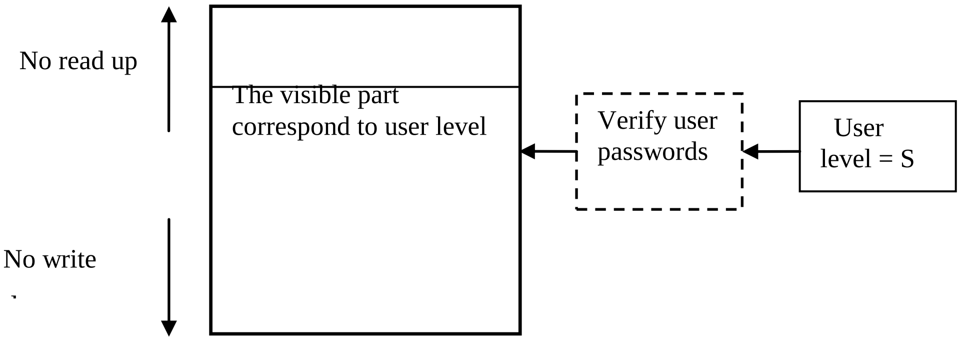

Figure 5. User at Level S

In TS (top secret) level, the data at this top level have the highest degree of secrecy which has to be verified users try accessing it with three passwords. The data at this level will be encrypted before being stored in the cloud. The third password based on image sequencing password with RSA algorithm to enhance the security of cloud confidential data.

Suppose four images have been used and fixed as a password. In this case the sequence number will be (for example 2468). So when we enter the sequence number, we get access to enter our cloud. Apparently, this sequence will always be changed whenever the system is logged on so that the password sequence is same but the position changes and that the numbers are changed. Next time the position of the images are shuffled hence password is also changed. The new password become (for example 4865) according to the position of the images the user choose at first. So this process consecutively happens and makes the password unbreakable.

As described earlier RSA will be used for data encryption to increase data security, as shown in Figure 6.

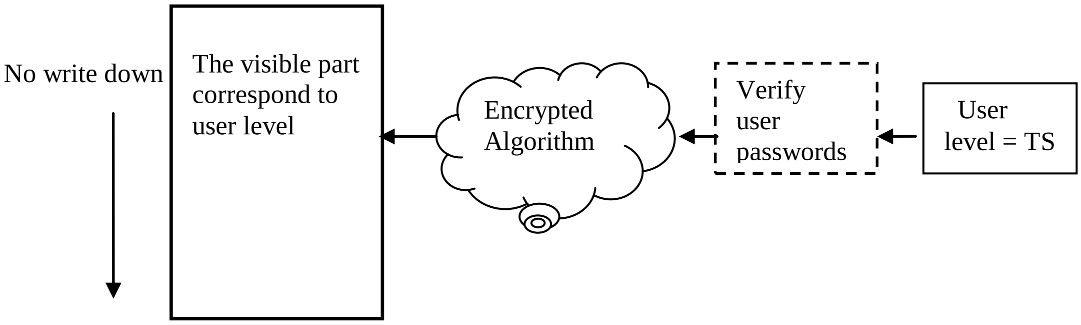

Figure 6. User at Level TS

The proposed model starts when a user enters his name and the first password (textual password) as described in Figure 7. The system verifies the user password, if the user level equal C, display the data at this level. If the user level higher than level C then the user needs to enter biometric password. The same process is done for the user in level S by entering two passwords textual and biometric. Then the scheme verifies the user passwords, if the user level equal S, display the data in this level and the lower level. However, if the user level higher than S level get the user third password. Then the proposed scheme verifies the user passwords, if the user level equal TS. Decrypt and display the data in this level and display the lower levels data.

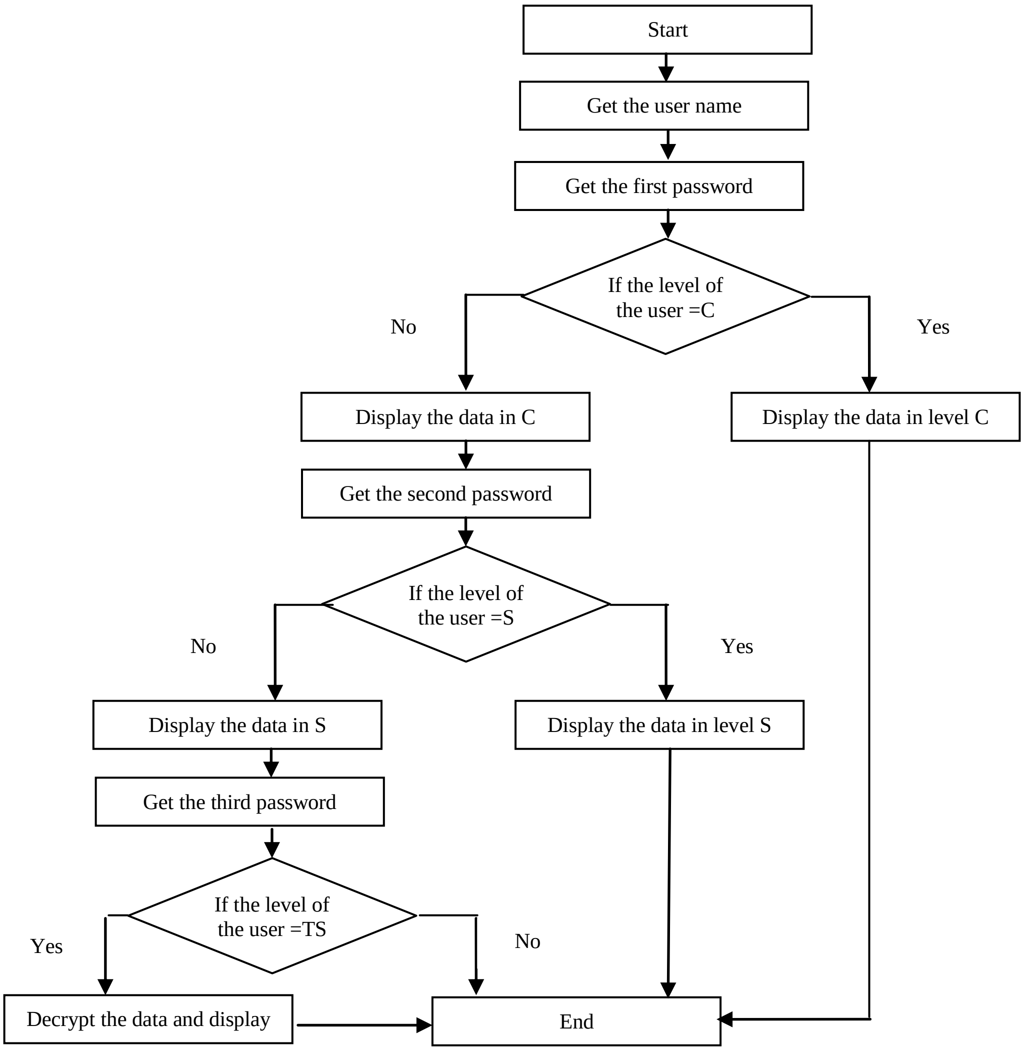
Start
Get the user name
Get the first password
If the level of the user =C
No
Yes
Display the data in C
Display the data in level C
Get the second password
If the level of the user =S
No
Yes
Display the data in S
Display the data in level S
Get the third password
If the level of the user =TS
Yes
No
Decrypt the data and display
End

Figure 7. The Steps for the Proposed Multilevel Authentication Scheme

5. Results and Discussions

The proposed scheme is based on three levels of authentication based on the levels of user data. The proposed scheme uses three types of passwords textual, biometric, graphical passwords and encryption layer. Hence, the scheme applies the defense in depth discipline as there are more than one layer of data protection. Moreover, the proposed scheme tries to overcome the limitations of different types of passwords by using more than one type of passwords such as textual, biometric and graphical passwords. As a final layer of protection, encryption is used to encrypt data that needs higher protection. Comparison between proposed scheme, Hao et al.'s scheme[16] and and Jaidhar C. D[10] in terms of security properties has been developed as described in Table 1.

Table 1: A Comparison between the Proposed Scheme and Two State of Art Schemes

Security Properties	Hao et Scheme	Jaidhar	Proposed Scheme
User is allowed to choose and change the password	Yes	Yes	Yes
Provides mutual authentication	Yes	Yes	Yes
Resists replay attack	Yes	Yes	Yes
Resists guessing attack	Yes	Yes	Yes
Resists parallel session attack	Yes	Yes	Yes
Resists reflection attack	Yes	Yes	Yes
Resists insider attack	Yes	Yes	Yes
Resists valid period extending attack	Yes	Yes	Yes
Resists impersonation attack	No	Yes	Yes
Resists DoS attack	No	Yes	Yes
Free from server involvement during password change	No	Yes	Yes
Provides early wrong password detection	No	Yes	Yes
Provides early wrong identifier detection	No	Yes	Yes
Provides secure session key generation	No	Yes	Yes
Use different types of passwords	No	No	Yes
Divides data into different security level	No	No	Yes
Support Encryption	No	No	Yes

As we can see in Table 1 in the three schemes users are allowed to change passwords and the three schemes are resisted to replay attach, guessing attack, parallel session attack, reflection attack, insider attack and valid period extending attack. The proposed scheme and Hao et scheme [16] cannot be hacked using DoS attack as the two schemes uses authentication method that is resistant to DoS attack because they have three passwords. However, the scheme described in [16] has three passwords but with same type. On the other hand, the propsed scheme has three passwords but with different types textual, biometric and graphical passwords. The different types of passwords make it difficult to break the system. Furthermore, the proposed scheme supports encryption for the top sensitive data. Moreover, the proposed scheme is the only scheme that divides the data into three levels based on it is sensitivity.

6. Conclusion

Authentication is one of the main important challenges in security of cloud computing. Single level authentication has many problems mainly with sensitive data, as passwords are easy to break. The proposed scheme provided additional layer of security and represents a solution for enhancing authentication system based on multilevel authentication. The proposed scheme consists of three level of authentication, and the data is split to these levels depending on the sensitivity to confidential (C), secret (S), and top secret (TS). Data at level (C) have the lowest sensitivity. The user at this level has single textual password to access this level data. The user at level (S) has two passwords, textual and biometrics password to access this level and the lower level. User at level (TS) has three password textual, biometrics password and image sequencing password. The data at this level is the more sensitive data so it is encrypted using RSA algorithm before storing in cloud database. A comparison analysis between the proposed scheme and two other state of the art schemes has been conducted. The initial results of the proposed scheme were very promising.

References

[1] J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security: CRC press, 2016.

[2] A. Yousif, M. Farouk, and M. B. Bashir, "A Cloud Based Framework for Platform as a Service," in Cloud Computing (ICCC), 2015 International Conference on, 2015, pp. 1-5.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[4] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 843-859, 2013.

[5] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," Telecommunications Policy, vol. 37, pp. 372-386, 2013.

[6] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST special publication, vol. 800, pp. 10-11, 2011.

[7] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud authentication based on anonymous one-time password," in Ubiquitous Information Technologies and Applications, ed: Springer, 2013, pp. 423-431.

[8] H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," in 2012 International Conference on Computing, Communication and Applications, 2012, pp. 1-4.

[9] B. Zwattendorfer and A. Tauber, "Secure cloud authentication using eIDs," in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 2012, pp. 397-401.

[10] C. Jaidhar, "Enhanced mutual authentication scheme for cloud architecture," in Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013, pp. 70-75.

[11] O. S. Faragallah, E.-S. M. El-Rabaie, F. E. A. El-Samie, A. I. Sallam, and H. S. El-Sayed, Multilevel Security for Relational Databases: CRC Press, 2014.

[12] H. Zhao, M. Xing, J. Zhao, and H. Li, "Design and Implementation of Multilevel Secure Database Management Access Control," Journal of Applied Science and Engineering Innovation, vol. 2, pp. 223-225, 2015.

[13] S. Sudha and V. M. Viswanatham, "Addressing security and privacy issues in cloud computing," Journal of Theoretical and Applied Information Technology, vol. 48, pp. 708-719, 2013.

[14] Y. Patel and N. Sethi, "Enhancing Security in Cloud Computing Using Multilevel Authentication," International Journal of Electrical Electronics & Computer Science Engineering, vol. 1, 2014.

[15] F. A. Alsulaiman and A. El Saddik, "Three-dimensional password for more secure authentication," IEEE Transactions on Instrumentation and measurement, vol. 57, pp. 1929-1938, 2008.

[16] Z. Hao, S. Zhong, and N. Yu, "A time-bound ticket-based mutual authentication scheme for cloud computing," International Journal of Computers Communications & Control, vol. 6, pp. 227-235, 2011.